RANDOM NUMBER GENERATOR

Patent number:	JP62144243
Publication date:	1987-06-27
Inventor:	OKAMOTO EIJI
Applicant:	NIPPON ELECTRIC CO
Classification:	
- international:	G06F7/58; H03K3/84
- european:	
Application number:	JP19850286494 19851218
Priority number(s):	JP19850286494 19851218

Abstract of **JP62144243**

PURPOSE:To improve the safety of a random number generator by dividing all outputs of a linear random number generating means into N pieces to apply the nonlinear conversion to all bits in each divided bit and combining the output bits for production of random numbers. CONSTITUTION:The output bits of shift registers of M-series generators 201, 202 and 203 serving as linear random number generators are used as addresses for the output of a single bit through ROM 211, 212 and 213 respectively. Then the ROM 211 or 213 is selected by a switch 223 with dependence on the exclusive OR between two bits of the outputs of registers in both generators 201 and 203 as well as the ROM 212. Then the exclusive OR between the output of the switch 223 and a bit of the output of the register in the generator 202.

---

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭62－144243

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和62年(1987)6月27日
G 06 F 7/58		6798－5B	
H 03 K 3/84		8626－5J	

審査請求　有　発明の数 1　(全2頁)

⑤4発明の名称　乱数発生器

②1特　願　昭60－286494

②2出　願　昭60(1985)12月18日

⑦2発明者　岡本　栄司　東京都港区芝5丁目33番1号　日本電気株式会社内

⑦1出願人　日本電気株式会社　東京都港区芝5丁目33番1号

⑦4代理人　弁理士 内原　晋

明細書

発明の名称　乱数発生器

特許請求の範囲

乱数を発生する乱数発生器において、1ビット又は複数ビットから成る乱数を生成する1つ又は複数の線形乱数生成手段と、前記1つ又は複数の線形乱数生成手段の全出力ビットをN(Nは正整数)個に分割して各分割内の全ビットを非線形変換するN個の非線形変換手段と、前記N個の非線形変換手段の出力ビットを組合せて乱数を発生する組合せ手段と、から成ることを特徴とする乱数発生器。

発明の詳細な説明

(産業上の利用分野)

本発明はデータを暗号化あるいはスクランブルするための乱数発生器に関する。

(従来技術)

従来、乱数発生器としては、複数のM系列発生器(昭和54年発行、宮川、岩垂、今井著「符号理論」昭晃堂128,129頁参照)の出力ビットを論理積、排他的論理和、スイッチ等で簡単に組合せて乱数ビットを発生する方法が良く使われている。

(発明が解決しようとする問題点)

従来の乱数発生器では、組合せ回路に入力される複数ビットが線形乱数であるために暗号解読の面からは安全性が低いという問題点があった。本発明の目的はこの問題点を簡単な構成で除去することにある。

(問題点を解決するための手段)

上記問題点は次の構成から成る乱数発生器にて解決される。すなわち、乱数を発生する乱数発生器において、1ビット又は複数ビットから成る乱数を生成する1つ又は複数の線形乱数生成手段と、前記1つ又は複数の線形乱数生成手段の全出力ビットをN(Nは正整数)個に分割して各分割内の全ビットを非線形変換するN個の非線形変換手段と前記N個の非線形変換手段の出力ビットを組合せて乱数を発生する組合せ手段と、から成ることを特徴とする乱数発生器である。

(作用)

第1図は本発明の作用原理を示すためのブロック図である。図において、101,102,103は線形乱数発生器であり、111,112,113は非線形回路、121は組合せ回路である。各非線形回路の入力は線形乱数発生器内のシフトレジスタの出力ビットであり、これらの非線形回路の出力を簡単な組合せ回路で組合せて乱数ビットを出力する。非線形回路111,112,113により線形な乱数発生器の出力ビットが非線形となるので複雑な乱数となる。

(実施例)

第2図は本発明の実施例を示すためのブロック図である。ROM211,212,213は線形乱数発生器の一例であるM系列発生器201,202,203内のシフトレジスタの出力ビットをアドレスとして、該アドレスに記憶されている1ビットを出力する。スイッチ223はROM211と213の出力のいずれかをROM212とM系列発生器101及び103の中のレジスタの出力2ビットとの排他的論理和に依存して選択する。該スイッチ223の出力とM系列発生器202内のレジスタの出力1ビットの排他的論理和が乱数となる。ここに示した組合せ回路は1例である。ROMの各アドレスには0又は1を書き込むが、0と1の個数はほぼ等しいようにする。ROMの中味あるいはM系列発生器の初期値がキーとなる。

本実施例において、各ROMは例えば複数のROMとしてこれら複数のROMの全出力の排他的論理和を出力するように変更することもできる。これらの変更は本発明の範囲内に含まれる。

(発明の効果)

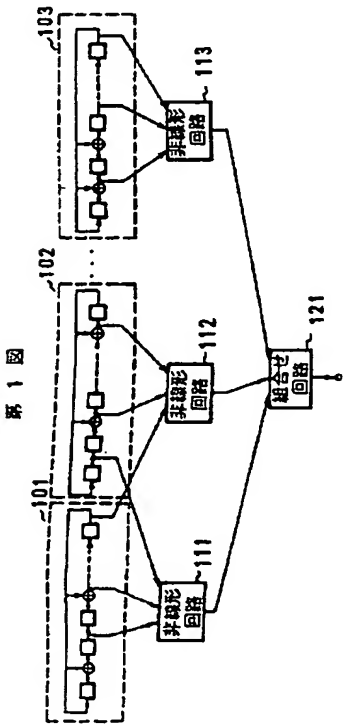
以上詳細に説明したように、本発明を用いれば安全性の高い乱数発生器を得ることができる。

図面の簡単な説明

第1図は本発明の作用原理を示すためのブロック図、第2図は本発明の実施例を示すためのブロック図である。図において、101,102,103は線形乱数発生器、111,112,113は非線形回路、121は組合せ回路、201,202,203はM系列発生器、211,212,213はROM、221,222は排他的論理和素子、223はスイッチを各々示す。

代理人 弁理士 内原

第1図



第2図